Reg. No. : | | | | | | | | | | | | |

Question Paper Code:U7202

B.E./B.Tech. DEGREE EXAMINATION, NOV 2025

Seventh Semester

Computer Science and Engineering

21UCS702-CRYPTOGRAPHY AND CYBER SECURITY

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	Define Model of network security.	CO1- U
2.	Compare Block and Stream cipher.	CO1- U
3.	Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm we have learned in arithmetic. Calculate q and r for a= -255 and n=11	CO2-App
4.	Find 117 mod 13.	CO2-App
5.	Prepare any one technique attacking in RSA.	CO1- U
6.	Give the applications of the public key cryptosystem.	CO1- U
7.	Create a simple authentication dialogue used in Kerberos.	CO1- U
8.	Define the term message digest.	CO1- U
9.	Which are the elements of cyber crime?	CO1- U
10.	List the privacy facts of web security problem.	CO1- U

PART – B (5 x 16= 80 Marks)

11.	(a)	Explain the Characteristics of Modern Cryptography and working Principle.	CO1- U	(16)
		Or		
	(b)	(i) Discuss the various security mechanisms.	CO1- U	(8)
		(ii) Summarize OSI security architecture model with neat diagram.	CO1- U	(8)

12.	(a)	What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example	CO1- U	(16)
		Or		
	(b)	Measure the Public key-distribution and Symmetric Key-Distribution	CO1- U	(16)
13.	(a)	Find the secret key shared between user A and user B using DiffieHellman algorithm for the following q=353; α (primitive root)=3, XA=45 and XB=50.	CO2- App	(16)
		Or		
	(b)	Perform encryption and decryption using RSA algorithm for p=17, q=11,e=7 m=88.	CO2- App	(16)
14.	(a)	How Hash function algorithm is designed? Explain their features and properties.	CO2- App	(16)
		Or		
	(b)	Apply the concepts involved in Signature generation and Verification functions of DSS.	CO2- App	(16)
15.	(a)	Apply the suitable of security algorithms using cryptography and cyber security for real time applications.	CO2- App	(16)
		Or		
	(b)	Analyze how Cross Site Scripting (XSS) help in the establishing a security framework for an organization.	CO3- Ana	(16)